Opciones de implementación de Seagate Instant Secure Erase

Documento de tecnología

Introducción

Cuando las unidades de disco duro se retiran y salen del centro de datos a manos de terceros, esto supone poner en alto riesgo los datos contenidos en esas unidades. No obstante, el departamento de informática aún debe retirar y deshechar regularmente las unidades por diversas razones, entre las que se incluye:

- Reutilización de las unidades para otras tareas de almacenamiento.
- Devolución de unidades por garantía, reparación o expiración de los contratos de arrendamiento.

La mayor parte de las unidades de disco duro quedan fuera del control de su propietario una vez que estas abandonan el centro de datos; de hecho, Seagate estima que diariamente se retiran del centro de datos alrededor de 50.000 unidades. Los datos corporativos y personales todavía residen en esas unidades, y cuando estas se retiran, aún es posible leer los datos allí almacenados. Incluso los datos que han sido eliminados de distintas unidades en todo un sistema de almacenamiento configurado con protección de datos RAID son vulnerables puesto que una sola tira en las matrices de alta capacidad de hoy en día es lo suficientemente amplia para almacenar cientos de nombres, números de seguro social y otros datos personales y sumamente delicados.

Complicaciones del control de unidades y costos de eliminación

En un esfuerzo por evitar la divulgación de datos y el posterior envío de las notificaciones para los clientes exigidas por las leyes de privacidad, las corporaciones han probado un sinfín de opciones para eliminar los datos en las unidades retiradas antes de que estas abandonen el lugar y puedan caer en manos inapropiadas. Los procedimientos de retiro actuales diseñados para impedir la lectura de los datos dependen en gran medida de la participación humana durante el proceso, por lo que están sujetos a fallas humanas y técnicas.

Los procedimientos de retiro utilizados actualmente presentan un gran número de desventajas de largo alcance:

- La sobreescritura de los datos en las unidades es costosa y bloquea recursos valiosos del sistema durante días. La unidad no genera ningún tipo de notificación al completar la tarea, y sobreescribir los datos no cubre los sectores reasignados en la unidad, lo cual deja los datos expuestos.
- Tanto la desmagnetización como la fragmentación física de una unidad son costosas. Es difícil garantizar que la fuerza desmagnetizadora sea la más óptima para el tipo de unidad, con lo que podrían quedar ciertos datos legibles en esta. La fragmentación física de la unidad pone en peligro el medio ambiente, y ninguno de los procedimientos permite devolver la unidad por garantía o expiración de arrendamiento.

Opciones de implementación de Seagate Instant Secure Erase

- Algunas empresas han concluido que la única manera de retirar las unidades de forma segura es guardarlas en su posesión y almacenarlas en depósitos por un tiempo indefinido. Sin embargo, este método no es realmente seguro, pues el gran número de unidades sumado a la participación humana inevitablemente conduce al extravío o hurto de algunas unidades. De hecho, un estudio de 2014 sobre el costo de la fuga de datos realizado por Ponemon Group reveló que la causa más común de la fuga de datos eran personas internas con intención dolosa o un ataque delictivo.
- Otras compañías prefieren contratar servicios profesionales para el proceso de eliminación, una opción costosa que implica el costo de desempeño y reconciliación de los servicios, así como de los informes internos y auditorías. Lo que es más preocupante, transportar una unidad al proveedor de servicios presenta otro riesgo, pues la unidad podría perderse o ser objeto del hurto en tránsito. El extravío de una sola unidad podría suponerle a la compañía millones de dólares para remediar la divulgación de los datos.

Los retos relacionados con el rendimiento, la escalabilidad y la complejidad han llevado a los departamentos de informática a rechazar las políticas de seguridad que requieran el uso de cifrado. Además, el cifrado ha sido visto como un procedimiento riesgoso por aquellos que no están familiarizados con la administración de claves, un proceso que le permite a una compañía asegurarse de que siempre pueda descifrar sus propios datos. Las unidades con cifrado automático (SED) resuelven estos problemas de manera integral, con lo que el cifrado para el retiro de unidades se hace fácil y asequible.

La tecnología Seagate Instant Secure Erase hace que el retiro de la unidad sea seguro, rápido y fácil

Las unidades SED codifican todos los datos del usuario a medida que ingresan en la unidad mediante una clave de cifrado de datos almacenada de forma segura en la misma. Por consiguiente, todos los datos almacenados en SED se codifican de forma predeterminada. Cuando llega el momento de retirar o reutilizar la unidad, el propietario simplemente envía un comando a la unidad para llevar a cabo la eliminación instantánea y segura Seagate Instant Secure Erase (ISE). El ISE de Seagate usa la capacidad de cifrado de las unidades SED para cambiar la clave de cifrado de los datos. Los métodos de borrado criptográfico, como Seagate ISE, ahora cuentan con el respaldo de ISO (Organización Internacional para la Normalización) y NIST (Instituto Nacional de Normas y Tecnología) como el método preferido para el borrado de datos porque “puede realizarse con un alto grado de garantía mucho más rápido que con otras técnicas de borrado”.[1] La eliminación cifrada segura remplaza la clave de cifrado de SED, como se muestra en la Figura 1.

Figura 1. El proceso de Seagate Instant Secure Erase

Una vez que se cambia la clave usada originalmente para cifrar los datos, los datos cifrados con esa clave se vuelven ilegibles e irrecuperables. De esta manera, el ISE de Seagate destruye de forma instantánea, segura y efectiva los datos almacenados en el dispositivo y la unidad queda lista para ser descartada, reutilizada o vendida. Las unidades SED, independientemente del enfoque de implementación, reducen los gastos operativos de informática al evitar los dolores de cabeza ocasionados por el control de unidades y los costos de eliminación. La seguridad de datos de nivel gubernamental de Seagate ayuda a garantizar que la privacidad esté conforme a las normas sin entorpecer la eficiencia informática.

Además, las unidades SED simplifican el proceso de desmantelar y preservar las inversiones de hardware para fines de devoluciones y reutilización al:

- Eliminar la necesidad de sobrescribir o destruir la unidad.
- Garantizar las devoluciones por garantía y vencimiento del arrendamiento.
- Permitir que se puedan reutilizar o vender las unidades con la garantía de que los datos anteriores no quedarán expuestos.

[1] ISO/IEC 27040 (Informática—Técnicas de seguridad—Protección de los datos almacenados); NIST 800-88 (Pautas de higiene de los medios)

Opciones de implementación de Seagate Instant Secure Erase

Soluciones de Seagate según las distintas necesidades de seguridad

- Hay dos tipos de unidades Seagate Secure disponibles. Los clientes pueden elegir la unidad SED estándar o los modelos con certificación Federal Information Processing Standard (FIPS 140-2) para mayor protección. Ambos tipos incluyen la función de borrado instantáneo y seguro Seagate Instant Secure Erase que permite a los clientes eliminar de manera rápida y segura el contenido de sus unidades en cuestión de segundos, una valiosa función que no tienen disponibles las unidades sin cifrado.

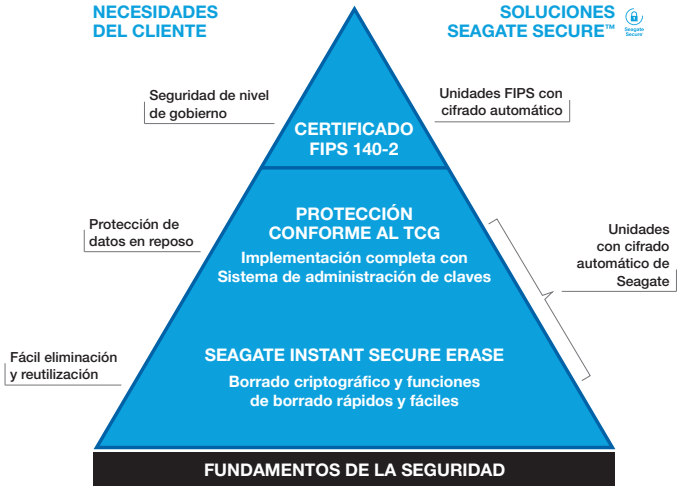

Figura 2. Soluciones Seagate Secure™ para todos los niveles de implementación de la seguridad

Cómo las unidades con cifrado automático (SED) de Seagate ejecutan el Instant Secure Erase

Las unidades SED de Seagate admiten más de una forma de ejecutar el ISE de Seagate, dependiendo del conjunto de comandos y configuraciones de la interfaz de la unidad. El método más seguro es utilizar la opción de borrado criptográfico disponible por medio del protocolo de seguridad Trusted Computing Group (TCG) de la unidad SED. Además de su seguridad superior, este método es fácil y rápido. Los clientes también pueden borrar sus unidades a través de los métodos de comandos de sobreescritura convencionales, pero estos se consideran en general menos seguros y pueden consumir mucho tiempo. En la tabla 1 se enumeran estos y otros métodos de borrado de datos. Tenga en cuenta que, en cualquier circunstancia, el controlador del host puede respaldar el ISE de Seagate a través de un comando compatible.

1. Las unidades configuradas con protección de datos en reposo, con o sin la protección avanzada antimanipulación de FIPS 140-2 llevan los protocolos de seguridad del TCG.

   Una unidad SED administrada con el protocolo de la especificación de almacenamiento del TCG permite un borrado criptográfico a nivel de bandas. Además de proteger los datos del usuario mientras la unidad se encuentra en uso, el ISE a nivel de banda de Seagate permite borrar todos o una parte de los datos almacenados en el dispositivo, sin afectar otras bandas de datos de la unidad. Este método de borrado electrónico requiere un software externo, disponible por medio de una gama de socios de Seagate.

   Una unidad SED administrada con el protocolo de la especificación de almacenamiento del TCG también puede borrarse por completo recurriendo al comando RevertSP del protocolo. Para este tipo de borrado seguro hace falta tener posesión física de la unidad a fin de leer el PSID (identificación segura física) de 32 caracteres que se encuentra en la etiqueta a fin de eliminar los datos de manera segura y configurar la unidad a su estado original de fábrica.

2. Las unidades que no estén configuradas con la protección de datos en reposo completa pueden habilitarse con los comandos de seguridad ATA.

   Para borrar una unidad SED de Seagate que esté configurada con el conjunto de comandos ATA se deberán activar los comandos ATA Security Erase Prepare (preparación para borrado de seguridad) y Security Erase Unit (unidad de borrado de seguridad). Cabe señalar que esta es una implementación única del ISE de Seagate.

Opciones de implementación de Seagate Instant Secure Erase

En la tabla 1 se muestra un resumen de los distintos métodos de borrado de datos de un SED. Véanse las notas que le siguen a la tabla.

Tabla 1. Opciones de Seagate Instant Secure Erase

Configuración inicial	Protección de datos en reposo, con o sin protección ante evidencia de manipulación		Seguridad limitada activada	Seguridad no activada
Método de eliminación	**Protocolo de seguridad TCG** Borrar	**Protocolo de seguridad TCG** RevertSP	**Seguridad ATA** Comandos Security Erase Prepare (preparación para borrado de seguridad) y Security Erase Unit (unidad de borrado de seguridad).	**Eliminar** Configuración/Comando de eliminación
Configuración compatible	Unidades SED de Seagate con almacenamiento TCG	Unidades SED de Seagate con almacenamiento TCG	Unidades SED SATA de Seagate	Unidades SED SATA y SAS de Seagate compatibles
Alcance del borrado	Eliminación cifrada a nivel de banda	Se ejecuta una eliminación cifrada en toda la unidad	Se ejecuta una eliminación cifrada en toda la unidad	Se ejecuta una eliminación cifrada en toda la unidad
Efecto secundario	Desbloquea banda y reinicia la contraseña de banda	La unidad SED es restaurada al estado de fábrica predeterminado	Desbloquea unidad y desactiva seguridad ATA	No dispone de seguridad inicial para evitar borrado accidental
Control de acceso	Requiere autenticación mediante contraseña administrada por un host o predeterminada por el dispositivo	Requiere autenticación usando contraseña impresa (y código de barras) en la etiqueta de la unidad	Requiere autenticación usando contraseña(s) administrada(s) por un host	No autentificada por el diseño (si la unidad se encuentra bloqueada, esta deberá ser desbloqueada por el operador antes de la ejecución)
Ventajas	Protección de datos en reposo Validación FIPS 140-2 Nivel 2 Interfaz de administración de seguridad completa basada en las especificaciones de almacenamiento TCG	Protección de datos en reposo Validación FIPS 140-2 Nivel 2 Interfaz de administración de seguridad completa basada en las especificaciones de almacenamiento TCG	Seguridad a nivel de unidad La seguridad usa comandos de seguridad ATA estándar	Ofrece borrado seguro sin gastos de gestión (por ejemplo, no requiere administración de contraseña)
Comentarios	Requiere hardware o software compatible con TCG	Requiere la presencia física de la unidad SED para leer el código de seguridad de la unidad	Utiliza comandos de seguridad ATA estándar	Es posible que se borren datos erróneos o maliciosos debido a que el comando no cuenta con protección

Notas

1. En la mayoría de los casos, el método empleado para borrar de forma segura una unidad configurada con alto nivel de seguridad también se puede emplear con configuraciones de bajo nivel de seguridad. Por ejemplo, el protocolo RevertSP puede funcionar en una unidad configurada en modo ATA, suponiendo que esta también sea compatible con el conjunto de comandos TCG (la disponibilidad de seguridad puede variar en función del modelo de la unidad).
2. El término *protección de datos en reposo* se refiere a la capacidad que tiene una unidad de cifrado automático (SED) para ofrecer protección de alto nivel de los datos en una unidad que ha sido configurada para bloquear la interfaz de datos ante accesos no autorizados mientras se encuentra conectada a un entorno informático en funcionamiento.
3. La Norma federal para el procesamiento de información (FIPS), Publicación 140-2, es una norma de seguridad informática del gobierno de EE. UU. para autorizar módulos de cifrado. Lleva por nombre *Requisitos de seguridad para módulos criptográficos (FIPS PUB 140-2, por sus siglas en inglés)* y fue publicada por el National Institute of Standards and Technology (NIST, o Instituto Nacional de Normalización y Tecnología). Esta norma establece los requisitos de seguridad que debe cumplir un módulo criptográfico utilizado dentro de un sistema de seguridad que protege datos de clase *confidencial pero sin clasificar.* Las unidades Seagate FIPS llevan certificación de nivel 2 (manipulación aparente); puede encontrar más información (en inglés) en: http://www.seagate.com/files/www-content/solutions-content/security-and-encryption/en-us/docs/faq-fips-sed-mb605-3-1411us.pdf

Opciones de implementación de Seagate Instant Secure Erase

Cómo llevar a cabo un borrado instantáneo y seguro Seagate Instant Secure Erase en una unidad SED de Seagate

Existen diversas maneras de eliminar los datos actuales, según el tipo de SED y las opciones seleccionadas para borrar de forma segura el dispositivo. Están disponibles las siguientes soluciones:

- Software Seagate SeaTools™ para Windows: herramienta gratis para PC que permite diagnosticar dispositivos de almacenamiento conectados de forma interna y externa. El software SeaTools es compatible con ISE de Seagate. El software SeaTools se puede descargar en www.seagate.com en la pestaña Support and Downloads (soporte y descargas), bajo SeaTools – Diagnosis Software (software de diagnóstico).
- Aplicaciones de software de administración de claves externas de socios de seagate, como IBM (Tivoli Key Lifecycle Manager), Wave, Winmagic, etc.
- Solución a la medida o integrada a fin de integrar capacidades de Seagate ISE en sistemas o aplicaciones de alojamiento. Póngase en contacto con su representante de ventas de Seagate para más información.
- Los usuarios de sistemas Linux pueden usar HDPARM (utilidad de línea de comando para el sistema operativo Linux) si desean emitir sus propios comandos SATA.

Referencias

Especificaciones de almacenamiento TCG—
www.trustedcomputinggroup.org/developers/storage/specifications

Especificaciones ATA—
www.t13.org/

Especificaciones SCSI—
www.t10.org/

Software SeaTools de Seagate—
www.seagate.com/www/en-us/support/downloads/seatools

Seagate Secure®

seagate.com

AMÉRICA Seagate Technology LLC 10200 South De Anza Boulevard, Cupertino, California 95014, EE. UU., +1 408 658 1000
ASIA/PACÍFICO Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapur 569877, +65 6485 3888
EUROPA, ORIENTE MEDIO Y ÁFRICA Seagate Technology SAS 16-18 rue du Dôme, 92100 Boulogne-Billancourt, Francia, +33 1 41 86 10 00